

REMARKS

Claims 47, 49-64, and 66-75 are pending in the present application, claims 74 and 75 having been added herein. The Office Action and cited references have been considered. Favorable reconsideration is respectfully requested.

The Examiner and Supervisory Primary Examiner Mattis are thanked for courtesies shown during the personal interview on April 15, 2010. The amendments presented herein are made in accordance with the discussions during that interview, which are accurately reflected in the Examiner Interview Summary Record.

The specification is amended to correct typographical errors noted therein. No new matter is added.

Claim 68 was rejected under 35 U.S.C. §112, second paragraph. Claim 68 has been amended to correct this inadvertent error. Withdrawal of this rejection is respectfully requested.

During the interview, the Examiner expressed her concern that the term "substantially in real-time" as used in the independent claims was indefinite. As indicated in the Interview Summary Record, Applicant notes that a portion of the invention is performed in real-time, which is what is meant by "substantially" in the claims. To advance prosecution, Applicant has deleted the phrase "substantially in real-time." Applicant has added new claims 74 and 75 to recite that the enabling detection is performed in real-time.

Claims 47-52, 57-58, 63-68, and 70-73 have been rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Publication No. 2003/0212910

Reply to Office action of January 4, 2010

(“Rowland”). Claim 59 was rejected under 35 U.S.C. § 103 as being unpatentable over Rowland in view of Keir (U.S. Patent Application No. 2004/0078384). Claims 55-56 were rejected under 35 U.S.C. § 103 as being unpatentable over Rowland in view of Tonelli (U.S. Patent No. 5,821,937). Claims 53-54, 60-62, and 69 rejected under 35 U.S.C. § 103 as being unpatentable over Rowland in view of Thorpe (U.S. Patent No. 7,089,306). Applicant respectfully traverses these rejections.

Claim 47 recites a method of collecting information relating to a communication network and to substantially all nodes operating in said communication network. The method comprises enabling detection of data conveyed by one or more detected nodes operating in the communication network in a manner that is transparent to the one or more detected nodes, to yield detected data, thereby enabling detection of the data passively, and analyzing the detected data and data relating to the communication network to identify at least one of identified information and missing information. The data relating to the communication network comprises node identification data, identified information comprises at least one of nodal information relating to the one or more detected nodes and nodal information relating to the communication network, and the missing information comprises at least one of missing information regarding at least one of the one or more detected nodes and missing information regarding the communication network. The method also includes storing at least a part of the identified information on a storage device comprising a computer readable medium accessible thereto, and if the missing information is identified, then querying at least one of one or more nodes operating in the communication network for

the missing information provided at least partially from the storage device, to yield queried nodes, thereby enabling collection of the missing information actively. This is not taught, disclosed or made obvious by the prior art of record.

According to the present invention, a "smart" combination of passive and active network entities is provided, thereby enabling having a substantially real-time inventory of all nodes (*e.g.*, representing a specific asset/device) within the communication network.

According to one embodiment of the present invention, a network detector does not convey data to nodes in the communication network nor do the nodes convey data thereto. Thus, the network detector can operate passively in the communication network (page 14, line 15 to page 15, line 10). On the other hand, the query engine collects information relating to the network and/or to nodes therein by probing them. Thus, according to another embodiment of the present invention, the network detector can operate actively in the communication network (page 15, lines 5-10). Further, being transparent to the network, the network detector relies on the network's activity in order to detect data conveyed by nodes operating therein. It should be noted that unlike the query engine, the network detector is not required to transmit packets to nodes in the network in order to collect information relating thereto (page 15, line 28-31). Specifically, the network detector detects passively data about any network nodes through which data is sent. The detected data is analyzed, along with other information about the network, including data about the identity of nodes in the network (including those nodes which have not been transmitting information). If any information

is missing regarding any of the nodes detected, then those nodes are queried to obtain that missing information.

As a result, the present invention enables a dynamic detection of the substantially real-time inventory of all nodes within the communication network: the nodes may be detected either passively AND/OR actively.

Rowland discloses a method and system for reducing the false alarm rate of a network intrusion detection system (NIDS). However, according to Rowland, there is no knowledge regarding all elements operating on the network at any given time (page 1, paragraph [0007]: "... A lower false alarm rate is facilitated even though knowledge of the entire protected network is not required...", etc.). Further, in contrast to the present invention, Rowland teaches probing the network for the device OS related information always and in any circumstances upon receiving an alarm (e.g., Abstract, page 2, paragraphs [0021-0023], etc.), and according to the present invention, the network is queried for the missing information only if (and only when) it is required. Thus, Rowland does not teach enabling to have a substantially real-time inventory of all nodes within the communication network and maintaining the substantially real-time information regarding said all nodes.

Keir discloses a network vulnerability testing and reporting method and system. However, in contrast to the present invention, Keir does not teach providing a "smart" combination of passive and active network entities, thereby enabling having a substantially real-time inventory of all nodes within the communication network. Also, Keir does not provide any guidance as to how to achieve the specific form of the

Appln. No. 10/580,543
Amdt. dated **May 4, 2010**
Reply to Office action of January 4, 2010

claimed combination (see, *In re Kubin*, 561 F.3d 1351, 90 U.S.P.Q.2d 1417 (Fed. Cir. 2009)). Therefore, Keir would not have rendered the amended claims obvious.

Tonelli discloses a software implemented method for auditing a network by using more than one soft probes to discover topology, host and interface information on devices in the network. However, similarly to Keir, Tonelli does not provide any guidance as to how to achieve the specific form of the claimed combination. Therefore, Tonelli would not have rendered the amended claims obvious.

Thorpe discloses a method and apparatus to collect information of different types that characterize a business entity and consolidate all these different types of information about the hardware, software and financial aspects of the entity in a single logical data store. However, Thorpe also does not provide any guidance as to how to achieve the specific form of the claimed combination. Therefore, Thorpe would not have rendered the amended claims obvious.

For at least these reasons, Applicant respectfully submits that claims 47, 64, 72, and 73, are patentable over the prior art of record. None of the secondary references cited with respect to the dependent claims remedy the deficiencies noted above with respect to Rowland. Accordingly, Applicant also submits that the dependent claims are patentable in and of themselves and for the reasons discussed above with respect to the independent claims.

In view of the above amendment and remarks, Applicant respectfully requests reconsideration and withdrawal of the outstanding rejections of record.

Appln. No. 10/580,543
Amdt. dated **May 4, 2010**
Reply to Office action of January 4, 2010

Applicant submits that the application is in condition for allowance and early notice to this effect is most earnestly solicited.

If the Examiner has any questions, he is invited to contact the undersigned at 202-628-5197.

Respectfully submitted,

BROWDY AND NEIMARK, P.L.L.C.
Attorneys for Applicant(s)

By /Ronni S. Jillions/
Ronni S. Jillions
Registration No. 31,979

RSJ:me
Telephone No.: (202) 628-5197
Facsimile No.: (202) 737-3528
G:\BN\COH\cohn\Arkin2\Pto\2010-05-04Amendment.doc